DATA AND IT POLICY

A large amount of data at AVP is stored electronically and on paper. It is essential that this data is carefully stored, protected and transferred securely. The storing and transfer of all data must adhere to the standards set out in the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) 2018.

DATA PROTECTION PRINCIPLES

The person with overall responsibility for compliance with the GDPR ("Compliance Officer") shall be appointed by Trustees.

AVP is guided by the principles of the Data Protection Act 1998 and the GDPR. The definition of personal and sensitive data is as follows:

Personal data is any information from which a living individual can be identified, either directly or from other information which may be written or in another format – e.g. audio visual or photographic.

Sensitive data includes information relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual orientation, gender identity, and criminal proceedings and convictions.

If there is any doubt whether data would be classed as personal or sensitive, the Compliance Officer should be consulted.

Data subjects will be told what information is being collected, the purposes for which it will be used and whether it will be made available to anyone else. Data subjects will have the right to see the information held about them, with the exception of references for employees and volunteers supplied for them in confidence.

VOLUNTEERS AND STAFF

All AVP volunteers must sign the volunteer agreement form, which commits them to respect the confidentiality of personal and sensitive data and gives volunteers the opportunity to consent to the storage and appropriate dissemination of the their data.

All staff are required to read and agree to this policy before signing their contract of employment.

PAPER RECORDS

AVP offices should be locked when unattended.

Personnel records should be kept in locked files and the keys kept with the Chair of Trustees or a person designated by him or her, and a nominated member of staff/trustee with personnel responsibilities.

Papers containing personal and sensitive data, including but not limited to names or email addresses or postal addresses or prisoner numbers, and which are no longer required, must be shredded before being recycled.

DATA TRANSFER

Before any data is transferred the necessity of the transfer should be considered. Data should only be transferred when it is essential for the smooth operation of AVP. In particular, it must be noted that personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of data protection. Where necessary, permission should be sought before sharing an individual's data unless it is a legal requirement to share the data. This does not apply to individuals sharing their own data with each other even if that data is also held on the AVP Database.

ELECTRONIC DATA STORAGE

This information is held on remote servers and access to the data in terms of adding, deleting or updating records is restricted to two Data Administrators nominated by the Trustees in addition to the AVPB Database Manager. The relevant passwords are kept in a locked safe for emergency purposes.

Personal and sensitive data (as defined by the GDPR) should only be stored electronically for the legitimate purposes of AVP Britain. All such data must be password-protected.

Personal and sensitive data should be destroyed after a maximum period of one year from the date it was first stored, if it is no longer required for the legitimate purposes of AVP Britain.

Personal and sensitive data should be destroyed immediately if any persons to whom that data pertains write to the Chair of Trustees and ask for this to be done, except where the Chair of Trustees has a legal obligation to retain the data.

If data is to be transferred through memory sticks, CD-ROMs or transferred to portable, laptop or similar computers, then they must be password-protected or encrypted.

Data storage media containing personal and sensitive data, including but not limited to memory sticks, computers and CDs/DVDs, must be securely wiped of the data or destroyed before being discarded.

ACTION TO BE TAKEN IF DATA GOES MISSING

The Chair of Trustees must be informed immediately if any confidential or sensitive data goes missing. An immediate investigation will be launched to discover where the data has gone.

If it is found that the data has been received by an unauthorised individual it must be determined whether that individual has accessed the data. If that individual has, and the data was correctly encrypted, compressed and password protected it suggests that the individual has unlawfully accessed the data. In such situations, it might be appropriate to involve the police in the investigation.

The Chair of Trustees will consider whether any individuals need to be informed about the lost data - even if it is subsequently found. This might be necessary if there is a risk of personal data relating to individuals having been sent to the wrong person.

NEGLIGENT TRANSFER OF DATA

If an employee/volunteer has been negligent in transferring sensitive, confidential or personal data this might be considered a disciplinary matter.

RETENTION OF DATA AND RECORDS

All documents, electronic and other information generated by employees or volunteers in the course of their work are the property of AVP.

Information gathered whilst working for AVP should not be used for commercial or personal gain, or otherwise misused.

Employees or volunteers may not retain, without permission, any documents so generated and must surrender them on request of the Chair of Trustees and also upon leaving service.

DATA HELD ABOUT EMPLOYEES AND VOLUNTEERS

General Principles

Throughout involvement and for as long as one year following the ending of employment or volunteering, AVP will need to keep information for purposes connected with employment and volunteering.

The information held will be for AVP's management and administrative use only, but from time to time, AVP may need to disclose some information held about employees and volunteers to relevant third parties. AVP may also transfer information to another Group or Organisation, solely for purposes connected with an employee's career or the management of AVP's work.

AVP requires all employees and volunteers to comply with the GDPR in relation to information about other staff and volunteers. If an employee or volunteer is in a position to deal with personal information about other employees or volunteers, he or she will be given separate guidance on his or her obligations, and must ask if he or she is unsure.

Volunteer Database

AVP Britain holds information about all employees and volunteers (including facilitators) who have signed the volunteer agreement on a single database. At present this information is restricted to contact details and status details of individual in terms of DBS checks, training etc.

Other Data

It should also be noted that AVP might hold the following information about an employee and sometimes a volunteer, for which disclosure to any person will be made only when strictly necessary for the purposes set out below:

- an employee's health, for the purposes of compliance with our health and safety and our occupational health obligations
- for the purposes of HR management and administration, for example to consider how an employee's health affects his or her ability to do his or her job and, if the employee is disabled, whether he or she requires any reasonable adjustment to be made to assist him or her at work
- confirming an employee's right to work in the UK
- the administration of insurance, pension, sick pay and any other related benefits
- in connection with *unspent* convictions to enable us to assess an employee's suitability for employment.

Email Distribution Lists

The email addresses of all volunteers and facilitators will be added to one or more of the email distribution lists which are also managed by the Database Administrators. There are currently email lists for

- Volunteers
- Facilitators
- Lead Facilitators
- Trustees
- Operations Committee
- Regional Coordinators
- Northwest Volunteers
- London and Southeast contacts

After each Training for Facilitators workshop the Lead Trainer should ensure that all new facilitators are enrolled on the database and the facilitators email list. Regional Coordinators should notify the Database Administrators of any new volunteers who have signed a volunteer agreement.

Secure Part of Website

Everyone on the database automatically has access to the secure part of the website unless they indicate otherwise. Names, physical addresses, telephone numbers, email addresses and roles (e.g. volunteer, facilitator etc.) of everyone on the database are available on the secure part of the website, unless a person indicates otherwise. Access to the secure part of the web site is managed by the Database Administrators.

USE OF IT

Employees and volunteers are permitted to make reasonable and limited personal use of the Internet in their own time or in an emergency through the AVP system. There are, however, conditions imposed on this personal use, namely that computers owned by AVP must not be used to:

- Access sites, which contain material which is illegal, racist or otherwise discriminatory or pornographic.
- Download, send or forward material, which could cause offence. This includes but is not limited to defamatory material, communications, which could constitute harassment, or messages conflicting with the duties of the individual or with AVP policies, or which may harm the reputation of AVP
- Gamble.
- Undertake shares or securities dealings.
- Undertake transactions related to a personal business.
- Copy or download material that may infringe intellectual property rights.

DOWNLOADS

Viruses and similar problems can bring an entire computer network to a standstill. It is important, therefore, that all employees and volunteers are aware of the need to act responsibly and minimise the risk of this occurring. To help protect AVP's network, employees or volunteers must not download any documents on to a computer belonging to AVP without being confident that it comes from a legitimate source.

USE OF EMAILS

No offensive language should ever be used in e-mails:

- E-mails should not be copied to people inappropriately
- If an employee /volunteer receives an offensive e-mail this should be reported to his/her line manager. It should not be passed on to other employees or volunteers.

During an employee's or volunteer's absence (for holiday, sickness or any other reason) AVP reserves the right for an authorised person to access the employee's or volunteers AVP e-mail account. This is necessary to ensure that any work-related issues are addressed in a timely manner.

EMAIL USE FOR PERSONAL PURPOSES

Employees or volunteers may only use their work e-mail address for work purposes. They are not to send personal e-mails using this address.

STORAGE OF E-MAILS

The GDPR requires that information that is recorded is not excessive, is not kept for longer than necessary and is relevant. Employees and volunteers therefore, are required to archive their e-mails appropriately and to delete information that is no longer required.

PASSWORDS

Access to AVP's computers must be password protected. Employees and volunteers are required to use their passwords, and not put in place any process which bypasses the requirement for a password. Passwords must not be stored by the computer.

Employees and volunteers must ensure that their manager has a record of their most recent password. This is important to allow their e-mail account to be accessed, if required, during their absence.

Passwords must not be disclosed to any other person.

COPYRIGHT

Copyright rules do apply to articles on the Internet. Hence, care should be taken when using Internet information. If there is any doubt whether material can be used the Chair of Trustees should be contacted for specific advice.

AVPB WEBSITE

Routine updates to the website (e.g. workshop dates) may be made regionally by employees or volunteers authorised by Database Administrators.

MONITORING

AVP reserves the right to monitor the e-mail and internet use on any computer which belongs to AVP. However, this will only be done if in the Chair of Trustees' view there is reason to believe misconduct has taken place.

ACTION TO BE TAKEN IN THE CASE OF INAPPROPRIATE USE

If an employee is found to have used e-mail or the internet in an inappropriate manner disciplinary action may be taken. In severe cases, this could include summary dismissal, depending on the nature and severity of the offence. A volunteer may be asked to end their volunteering arrangement with AVP.

NOTES

Agreed by the Board 1 June 2018

Next review June 2019